DrinkerBiddle&Reath
LLP

Laura H. Phillips
202-842-8891
laura.phillips@dbr.com

Law Offices
1500 K Street, N.W.
Suite 1100
Washington, DC
20005-1209

202-842-8800
202-842-8465 fax
www.drinkerbiddle.com

PHILADELPHIA
NEW YORK
LOS ANGELES
SAN FRANCISCO
PRINCETON
FLORHAM PARK
BERWYN
WILMINGTON

July 20, 2004

Ms. Marlene Dortch
Secretary
Federal Communications Commission
445 Twelfth Street S.W.
Washington, D.C. 20554

Re: *Ex Parte* of RealNetworks, Inc. MB Docket No. 04-65;
In the Matter of Digital Output Protection Technology and
Recording Method Certifications, Helix DRM Trusted Recorder
and Helix Device DRM Technology

Dear Ms. Dortch:

On July 19, 2004, Todd Alberstone, Associate General Counsel, RealNetworks, Inc. ("RealNetworks") and Surya Mantha, General Manager, Marketing and Strategic Relations, RealNetworks and Laura H. Phillips, counsel for RealNetworks, met with Jordan Goldstein, Legal Advisor to Commissioner Copps regarding RealNetworks' digital output technology, Helix DRM Trusted Recorder and Helix Device DRM Technology as proposed by RealNetworks for certification to protect broadcast flagged marked content. The participants discussed the attached presentation provided by RealNetworks.

As required by Section 1.1206(b), as modified by the policies applicable to electronic filings, one electronic copy of this letter is being submitted for the above-captioned docket.

Respectfully submitted,

Laura Phillips

Laura H. Phillips
Counsel for RealNetworks, Inc.

LHP:css
Enclosure
cc: Jordan Goldstein (via e-mail)

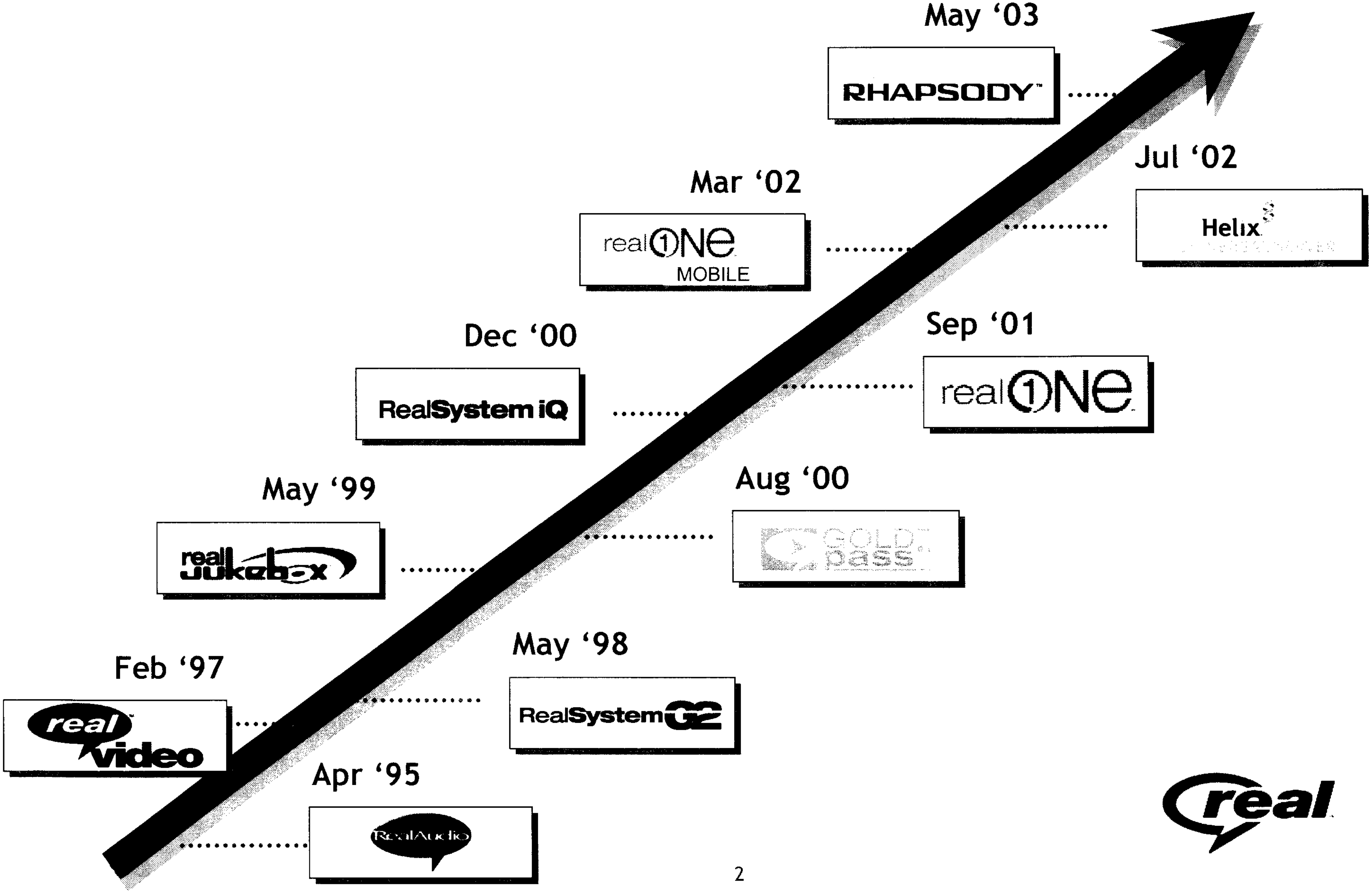
Established
1849

RealNetworks

Digital Output Protection Technology --
Helix DRM Trusted Recorder and
Helix Device DRM Technology

FCC Ex Parte Presentation
July 19, 2004
MB Docket No. 04-65

10 Years of Innovation



Apr '95
RealAudio

Feb '97
real video

May '98
RealSystem G2

May '99
real jukebox

Aug '00
GOLD pass

Dec '00
RealSystem iQ

Sep '01
real ONE

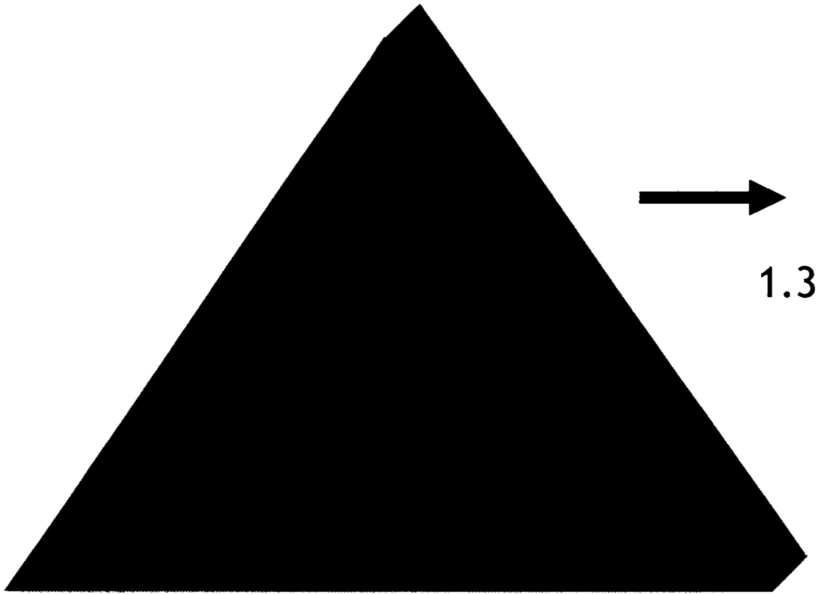
Mar '02
real ONE
MOBILE

Jul '02
Helix

May '03
RHAPSODY™

real

Real's Approach



1.3 Million Subscribers, Market Leader

Enable others to build digital media businesses

Technology

Servers Formats DRM Applications

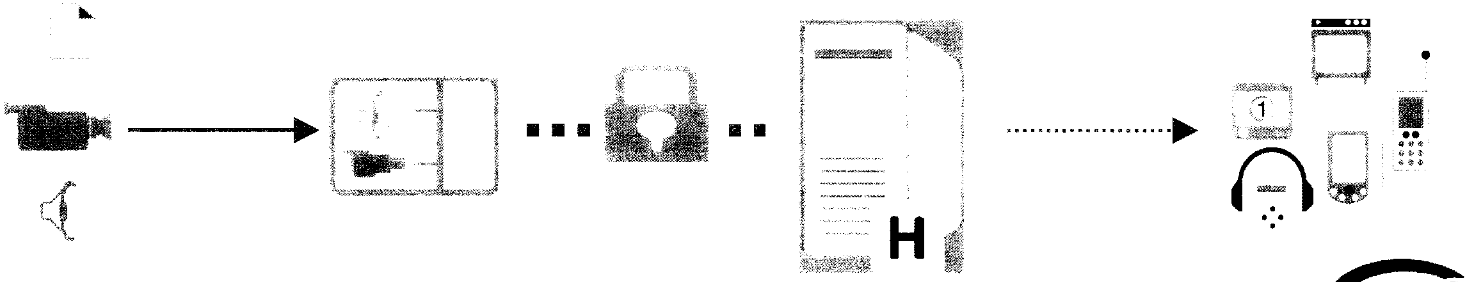
Core Media Delivery Components

Encoder: compresses media into small information packets.

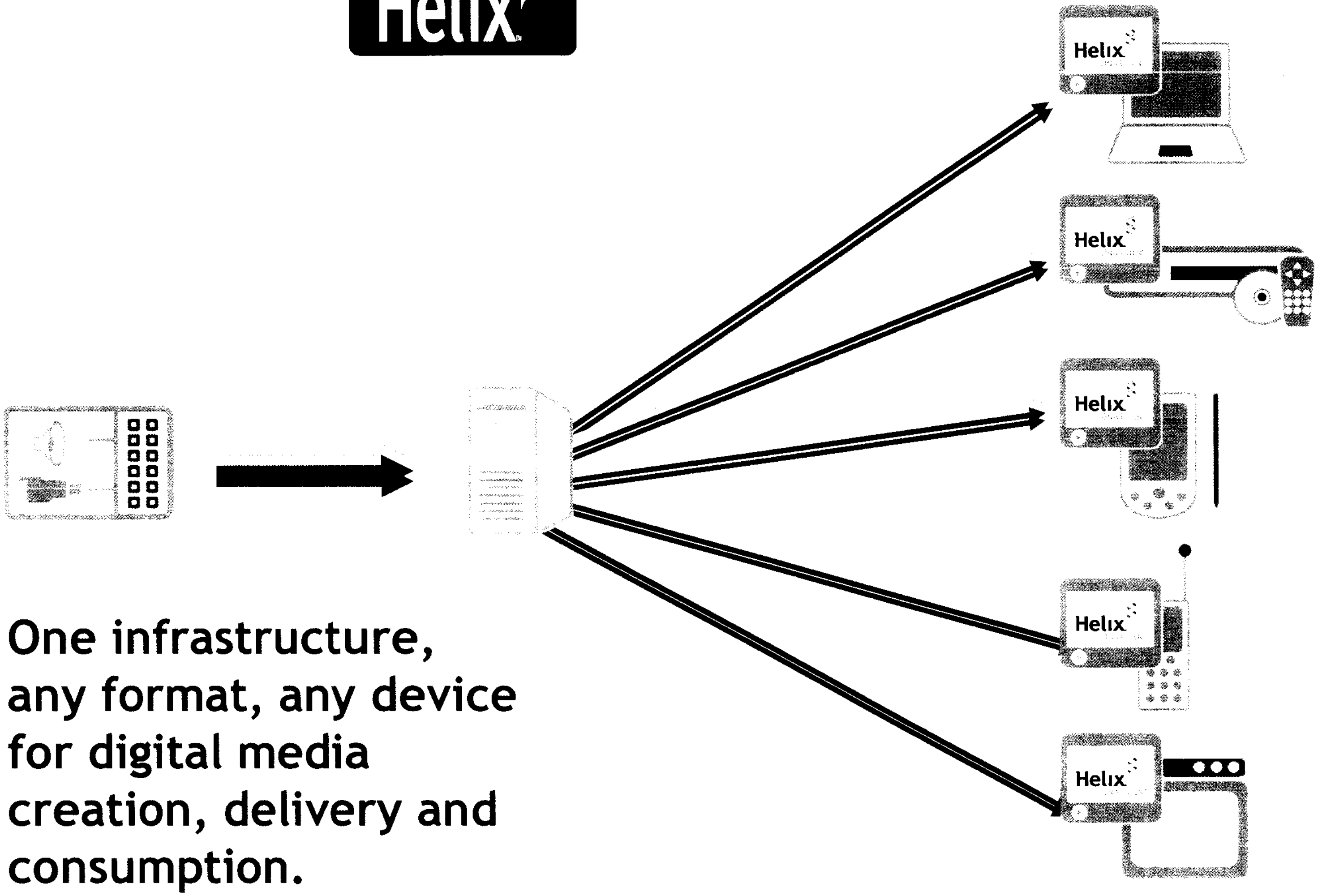
DRM: Protects content and applies business rules.

Server: Delivers content to devices.

Devices: Contain software or hardware applications that decode and plays content if authorized.

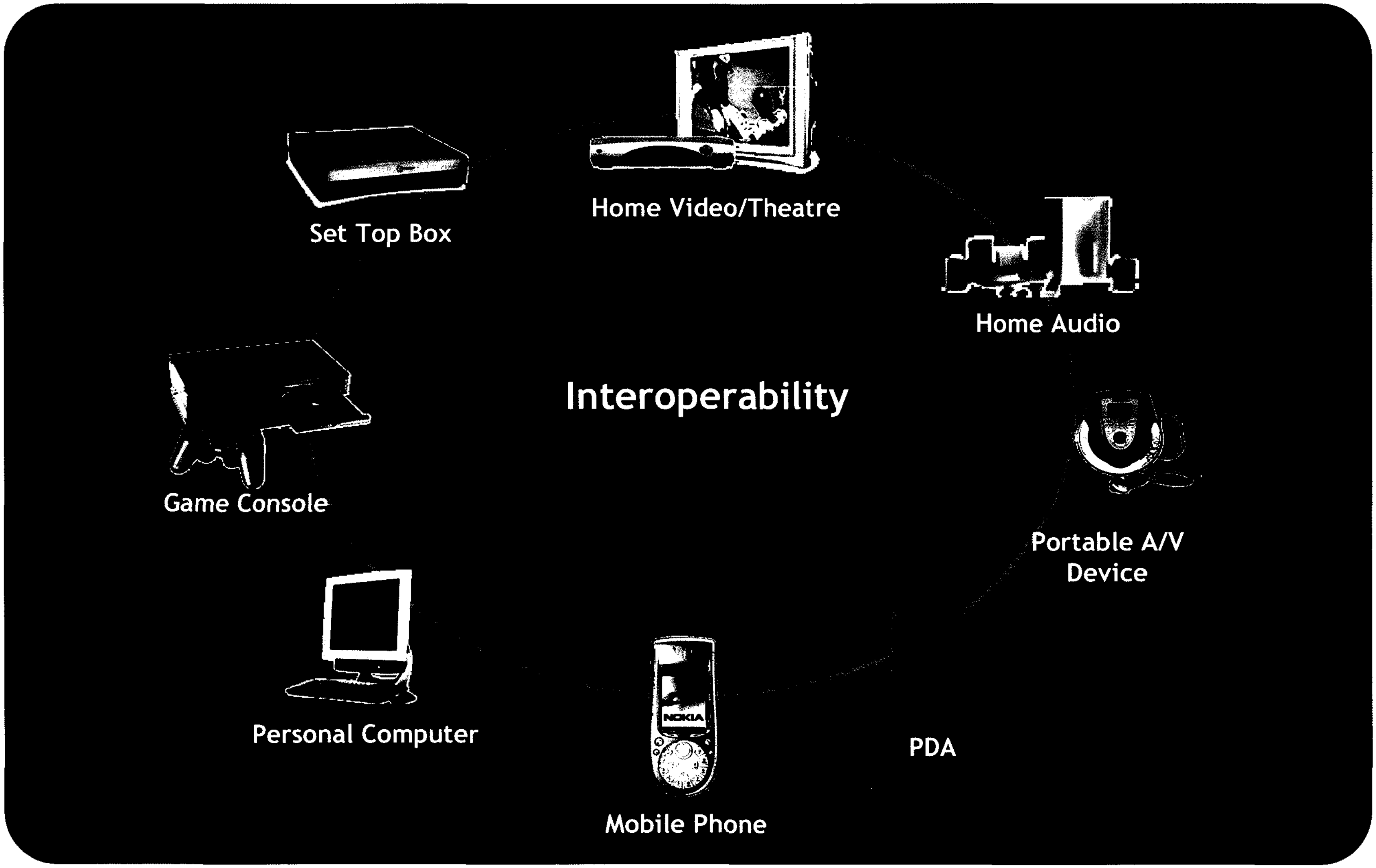


Helix



One infrastructure, any format, any device for digital media creation, delivery and consumption.

Goal: Interoperability Across Devices



Interoperability

Set Top Box

Home Video/Theatre

Home Audio

Portable A/V Device

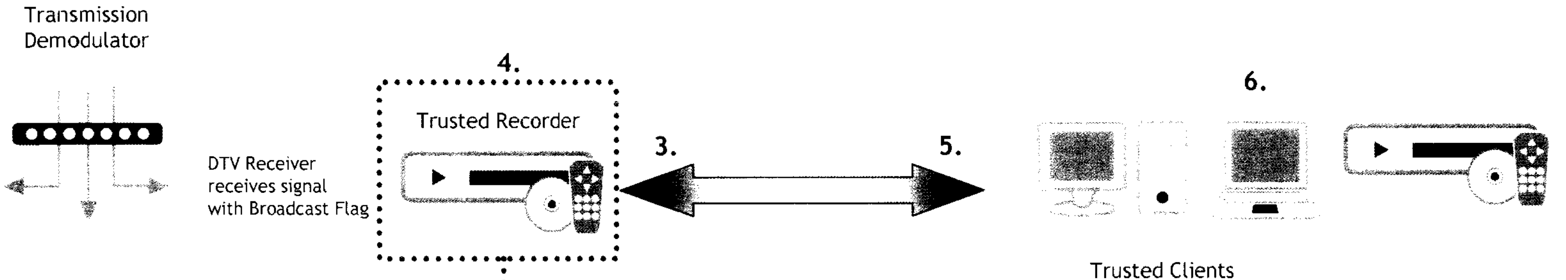
PDA

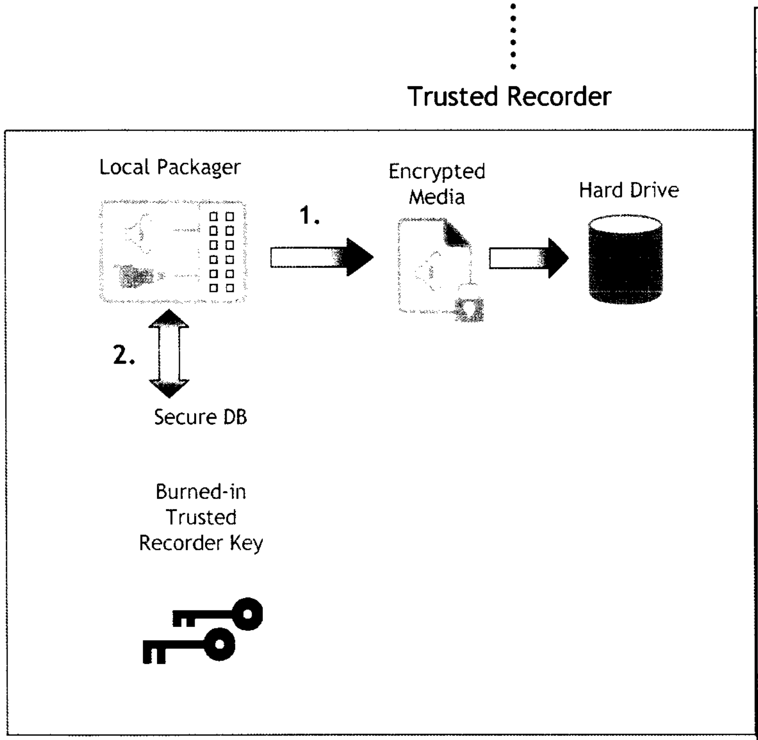
Mobile Phone

Personal Computer

Game Console

Helix DRM for Broadcast Flag - Technical Overview





Content Protection

1. Trusted Recorder encrypts Marked Content received from Demodulator with random Content Key
2. Trusted Recorder uses Trusted Recorder Key to encrypt Content Key and inserts encrypted Content Key into media file

Content Distribution

3. Trusted Client requests authorization to consume Marked Content by passing its Certificate containing a unique ID and unique Key
4. Trusted Recorder validates the Certificate if RTT, TTL and device limit parameters are met
5. Trusted Recorder encrypts its Trusted Recorder Key with the Trusted Client Key and sends it to the Trusted Client
6. Trusted Client can now consume any Marked Content originating from this Trusted Recorder

Helix DRM for Broadcast Flag - Technical Overview

- Helix DRM Trusted Recorder
  - Responsible for protecting Marked Content received from Demodulator and authorizing Trusted Clients
  - Can be a PC or STB implementation
  - Security level of Internet-based DRM solution with addition of proximity limitations
- Helix DRM Trusted Client
  - Allows for consumption of Marked Content in variety of products
  - Strict robustness and proximity requirements, beyond FCC requirements
- Protection of Marked Content
  - Strong cryptography for content encryption
  - Strong cryptography for device licensing
  - Enforcement through licensing agreements
  - Allows for revocation and renewability of both content and devices
- Distribution of Marked Content
  - Trusted Recorder authenticates Trusted Client before sending Recorder Key
  - Limits redistribution by authentication and by use of RTT, TTL and device limits

Helix DRM for Broadcast Flag - Policy Issues for Interim Certification

- Proximity Controls
  - RTT and TTL
  - Device limitations that mimic “home network” environment
- Licensing and Recognition of Downstream Devices
  - Licensing of Helix Device DRM technology on reasonable and nondiscriminatory terms
  - Commitment to cooperate with other broadcast flag technologies for the exchange of revocation information
- Compliance Rules
  - Contained in License Agreement and ongoing discussions with MPAA and other rights holders and industry groups
- Change Management
  - Will cooperate with content owners to devise process
  - Commit to ensure any new implementation that does not diminish protections against indiscriminate redistribution